Math 116: Problem Set 3

Owen Jones

1/29/2024

1. (a) There exist integers x, y s.t $17x + 101y = \gcd(101, 17)$
   $101 = 5 \cdot 17 + 16$
   $17 = 1 \cdot 16 + 1$
   $16 = 16 \cdot 1$
   $\Rightarrow 6 \cdot 17 - 1 \cdot 101 = 1$

   (b) $6 \cdot 17 \equiv 1 \pmod{101} \Rightarrow 6 = 17^{-1} \pmod{101}$

2. (a) $30 = 4 \cdot 7 + 2$
   $7 = 3 \cdot 2 + 1$
   $2 = 2 \cdot 1$
   $\Rightarrow 13 \cdot 7 - 3 \cdot 30 = 1$
   $\Rightarrow 7d \equiv 1 \pmod{30}$ for $d = 13$.

   (b) We want $D(E(m)) = m^{7 \cdot d} \equiv m \pmod{31}$. By Fermat's Little Theorem, $m^{31} \equiv m \pmod{31}$ $\forall m \in \mathbb{F}_{31}$. Let $D(m) = m^{24} \pmod{31}$.

3. (a) $12x + 236y = 28$ which is reducible to $3x + 59y = 7$
   $59 = 19 \cdot 3 + 2$
   $3 = 1 \cdot 2 + 1$
   $\Rightarrow 20 \cdot 3 - 59 = 1 \Rightarrow 140 \cdot 3 - 7 \cdot 59 = 7$
   $140 \equiv 22 \pmod{59}$
   $x = 22 + 59k$ gives all possible integer solutions.

   (b) There are no solutions because $12x, 236$ are both divisible by 4, so $\forall x$ 4 divides $12x \pmod{236}$. However, 4 does not divide 30.

4. (a) $30030 = 116 \cdot 257 + 218$
   $257 = 1 \cdot 218 + 39$
   $218 = 5 \cdot 39 + 23$
   $39 = 1 \cdot 23 + 16$
   $23 = 1 \cdot 16 + 7$
   $16 = 2 \cdot 7 + 2$
   $7 = 3 \cdot 2 + 1$
   $2 = 2 \cdot 1$
   Thus, $\gcd(30030, 257) = 1$.

   (b) 257 can be factored as a unique product of primes $\prod p_i$. Because 30030 and 257 are coprime, 257 is not divisible by any of $30030's$

factors. Moreover, 257 is not divisible by any prime up to 13. Consider what happens when we divide 257 by the next largest prime. Observe, $257 = 15 \cdot 17 + 2$. It follows that if we divide 257 by any prime 17 or larger, the quotient will be smaller than 17. Thus, 257 cannot be written as a product of 2 or more primes because 257 is not divisible by any prime less than 17. Hence, 257 must be prime.

5. (a) $4883 - 4369 = 514$
   $4369 = 8 \cdot 514 + 257$
   $514 = 2 \cdot 257$
   $\Rightarrow \gcd(4883, 4369) = 257$
   (b) $4883 = 19 \cdot 257$ and $4369 = 17 \cdot 257$.

6. (a) If $ab \equiv 0 \pmod{p}$ then $p|ab$. Since p is prime, and $p \mid ab$ then either $p \mid a$ or $p \mid b$. Because $p \mid a$ or $p \mid b$ then either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$
   (b) If $\gcd(n, a) = 1$ then there exists integers s, t s.t $sn + at = 1$. Multiplying both sides by b we obtain $snb + abt = b$. Because $b - abt = snb$, $n \mid b - abt$. Thus, $b \equiv abt \pmod{n}$. However, we know $n \mid ab \Rightarrow abt \equiv 0 \pmod{n}$. Hence, we $b \equiv 0 \pmod{n} \Rightarrow n|b$.

7. Let $p \geq 3$ be prime and suppose $x^2 \equiv 1 \pmod{p}$. It follows $p|x^2 - 1 \Rightarrow p|(x-1)(x+1)$ by difference of squares. By $6a$, we obtain $p|x - 1$ or $p|x + 1$. Hence, either $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$ Thus,

8. Case 1: $p \mid a$
   $a \equiv 0 \pmod{p} \Rightarrow a^p \equiv 0^p \pmod{p} \Rightarrow a^p \equiv 0 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$.
   Case 2: $p \nmid a$
   Let $x, x' \in \mathbb{F}_p$. It follows $\exists y, y' \in \mathbb{F}_p$ s.t $ax \equiv y \pmod{p}$ and $ax' \equiv y' \pmod{p}$. If $y = y'$, then $p \mid a(x - x') \Rightarrow p \mid (x - x') \Rightarrow x = x'$. Thus, $\{0a, a, 2a, \ldots, a(p-1)\}$ is just a permutation of $\mathbb{F}_p$. Observe $0a \equiv 0 \pmod{p}$. It follows by multiplying all the non-zero elements together we obtain $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Because p and $(p-1)!$ are relatively prime, $(p-1)!$ has a multiplicative inverse, so $a^{p-1} = 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$.

9. By Fermat's Little Theorem, $2^{100} \equiv 1 \pmod{101} \Rightarrow 2^{10200} \cdot 2^3 \equiv 2^3 \pmod{101}$. Thus, $2^{10203} \equiv 8 \pmod{101}$

10. 7958357

11. (a) $x = 142032116757, y = -466560018663026$
    (b) $313608160045 * 563608596325677 \equiv 1 \pmod{1030168614988703}$
    (c) $343390387426778 * 313608160045 + 9620549844273 \equiv 2228097317981 \pmod{1030168614988703}$
    $\Rightarrow x = 313608160045$

In [2]:
```
import math as m
import numpy as np
```

In [25]:
```
def extended(a, b):
    x_0,y_0, x_1,y_1 = 0,1, 1,0
    while a != 0:
        q, r = b//a, b%a
        m, n = x_0-x_1*q, y_0-y_1*q
        b,a, x_0,y_0, x_1,y_1 = a,r, x_1,y_1, m,n
    gcd = b
    return gcd, x_0, y_0
#used article from brilliant to help write the function
```

In [26]:
```
extended(313608160045,1030168614988703)
```

Out[26]: (1, -466560018663026, 142032116757)

In [13]:
```
313608160045*(-466560018663026)+1030168614988703*142032116757
```

Out[13]: 1

In [14]:
```
x=1030168614988703-466560018663026
```

In [15]:
```
x
```

Out[15]: 563608596325677

In [16]:
```
(313608160045*563608596325677)%1030168614988703
```

Out[16]: 1

In [17]:
```
2228097317981-9620549844273
```

Out[17]: -7392452526292

In [18]:
```
egcd(313608160045,1030168614988703)
```

Out[18]: (1, -466560018663026, 142032116757)

In [19]:
```
-466560018663026+1030168614988703
```

Out[19]: 563608596325677

In [20]:
```
142032116757-313608160045
```

Out[20]: -171576043288

In [21]:
```
313608160045*563608596325677-171576043288*1030168614988703
```

Out[21]: 1

In [22]:
```
563608596325677*(-7392452526292)%1030168614988703
```

Out[22]: 343390387426778

In [23]:
```
(343390387426778*313608160045+9620549844273)%1030168614988703
```

Out[23]: 2228097317981

In [ ]: